JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 34, 1015-1030 (2018)
DOI: 10.6688/JISE.201807_34(4).0013

End-to-end Congestion Relief and Physical Layer Security-Aware Routing Design for Ad Hoc Networks in IoT Applications*

YANG XU[1], JIA LIU[2,3], RUO ANDO[2] AND NORIO SHIRATORI[4]
[1]*School of Economics and Management*
Xidian University
Xi'an, 710071 P.R. China
[2]*Center for Cybersecurity Research and Development*
National Institute of Informatics
Tokyo 101-8430, Japan
[3]*State Key Laboratory of ISN*
Xidian University
Xi'an, 710071 P.R. China
[4]*Research Institute of Electrical Communication*
Tohoku University
Sendai 980-8577, Japan
E-mail: yxu@xidian.edu.cn; {jliu; ruo}@nii.ac.jp; norio@shiratori.riec.ac.jp

Ad hoc networks are important pillars for IoT (Internet of Things) development. In order to support IoT traffic transmission in ad hoc networks, it is of great importance to design effective routing protocols to relieve traffic congestion while ensuring data secrecy. To this end, in this paper we first propose a physical layer security-aware congestion relief routing protocol (PCRR). Through sensing the eavesdroppers' location, hop count and congestion information of available paths, PCRR can select an appropriate secure route for data transmission. Based on PCRR and combining the advantages of single-path and multi-path routing strategies, we further develop a mixed-path PCRR protocol (M-PCRR), which is more capable of counteracting eavesdroppers by utilizing the simultaneous transmissions from multiple paths. According to the current network state information, M-PCRR can flexibly decide whether or not to execute the multi-path scheme. Finally, we conduct extensive OPNET simulations to validate the performance of proposed routing protocols and show how their route selection is conducted. The results indicate that compared with AODV, PCRR and M-PCRR can improve the network throughput, reduce the hop count and energy consumption, while ensuring the delay performance and control overhead.

Keywords: ad hoc networks, routing design, congestion relief, physical layer security, IoT

1. INTRODUCTION

In the near future, there will be billions of sensor-enabled intelligent devices which connected by the Internet, composing a huge network typically known as Internet of Things (IoT) [1-4]. With the concept of "anything connected anytime" in IoT, it will bring immense potentially new products and services in many different domains, such as

Received August 31, 2017; revised October 31, 2017; accepted December 15, 2017.
Communicated by Xiaohong Jiang.
* A conference version of this work has been accepted by the International Conference of NaNA2017, which was held in Kathmandu City, Nepal, Oct.16-19, 2017.

smart homes, smart grid, e-health, e-learning, industrial automation, intelligent transportation and logistics. Consequently, traffic from wireless and mobile devices will account for much more proportion of total IP traffic, and will be up to about 63% by 2021 [5]. Though IoT will make the quality of citizens' life improved, it encounters tremendous challenges of heavy traffic congestion and serious eavesdropping [6-8]. Therefore, to promote the commercialization and application of IoT, traffic congestion relief and protecting data secrecy are of great significance.

Ad hoc networks are important pillars for IoT development [9], which support IoT traffic transmission in a self-organized manner [10, 11]. Ensuring the secrecy of user messages is challenging in ad hoc networks due to both the open nature of wireless channel and the lack of centralized administration. The traditional cryptographic-based approach can not be easily applied in a resource-limited ad hoc network since not only it incurs high computing complexity and energy consumption [12], but also it is extremely complicated to conduct key management and spreading. As a complement of cryptography, the physical layer security technique, an information-theoretic approach which exploits the fundamental characteristics of wireless channel to achieve perfect secrecy, is expected to be a promising solution to guaranteeing security for ad hoc networks and thus has attracted considerable attention from both academic and industrial communities [13, 14].

Routing protocols, which determine the end-to-end path(s) for traffic in ad hoc networks, have critical impacts on the fundamental network performance which includes throughput, delay, packet loss and so on [15, 16]. Some classical routing protocols have been proposed for ad hoc networks, such as AODV [17], DSR [18], OLSR [19], *etc.* However, routing design with the consideration of physical layer security is still largely uninvestigated and there only have some initial results [20-26]. Specifically, Saad *et al.* employed a tree-formation game to choose secure paths in multi-hop wireless ad hoc networks [20]. Ghaderi *et al.* explored the routing design for multi-hop ad hoc networks to guarantee transmission security with minimum energy consumption [21]. Yao *et al.* investigated the physical layer security-aware routing with decode-and-forward relaying scheme [22], and Lee proposed an optimal power allocation strategy for maximizing the secrecy rate in a special multi-hop relay network with single source-destination pair [23]. More recently, Xu *et al.* studied the QoS (quality of service)-security tradeoffs for routing design in ad hoc networks [24-26].

It is notable that, however, all the above routing protocols belong to the single-path routing. As evident from previous studies [27, 28], compared with single-path routing, multi-path routing has more potential to relieve end-to-end traffic congestion in many network scenarios including IoT applications [2]. This is mainly because that multi-path routing can distribute traffic on multiple paths to achieve a better load balancing. Motivated by this, in this work we will apply the multi-path routing strategy which can balance the traffic load in the whole network, and meanwhile degrade eavesdroppers' channel conditions by simultaneous transmission of multiple paths. As a popular saying goes, every coin has two sides. Multi-path routing strategy achieves its benefits at the cost of more routing overhead and more collisions on MAC layer. Without the consideration of security, a comprehensive comparison between the performance of single-path and multi-path routing protocols in ad hoc networks has been reported in [29, 30]. Some insights for the practical development of ad hoc networks can be concluded as follows:

- In the case that the path length (in terms of hop count) between a pair of source node and destination nodes is relatively short, *e.g.*, about 2 or 3 hops, the performance of single-path routing is similar to that of multi-path routing.
- In the case that the path length is medium, *e.g.*, about 4 or 5 hops, the performance of single-path routing could be better than that of multi-path routing, especially when the traffic load is light.
- In the case that the path length is relatively long, *e.g.*, more than 6 hops, the performance of multi-path routing is better than that of single-path routing, especially when the traffic load is in heavy.

Inspired by the above analysis, in this study we first propose a single-path routing protocol termed as physical layer security-aware congestion relief routing (PCRR). PCRR selects an optimal path for data transmission with the considerations of eavesdroppers' location, path length (hop count) and congestion status, which can improve the network security and performance. Based on PCRR, we further propose a mixed-path PCRR routing protocol (M-PCRR). By collecting and analyzing current network state information, M-PCRR determines whether or not to activate the multiple path mechanism. When there is no eavesdropper or path length is short and the traffic is not overloaded, M-PCRR adopts the single-path routing strategy; on the contrary, the multi-path routing mechanism is executed. Finally, we conduct extensive OPNET simulations to validate the performance of proposed routing protocols.

The remainder of this paper is organized as follows. The preliminaries involved in this paper are presented in Section 2. We show the details of designing PCRR and M-PCRR in Section 3 and Section 4, respectively. Section 5 provides the simulation results, and Section 6 concludes this paper.

2. PRELIMINARIES

In this section, we first present the system model and introduce the network secure performance from the perspective of physical layer security.

We consider a general multi-hop ad hoc network which consists of arbitrarily distributed (legitimate) nodes and possible (malicious) eavesdroppers. A K-hop path (route) $\Pi = \langle l_1, \ldots, l_K \rangle$ in the network consists of K links from l_1 to l_K, and a link $l_k \in \Pi$ connects two legitimate nodes S_k and D_k on path Π. The decode-and-forward (DF) relaying scheme [31, 32] and the standard narrow band fading channel model [33] are also employed in our study. With this model, the wireless channel between any pair of nodes X and Y is characterized by the large-scale path loss along with the small-scale Rayleigh fading, and the fading coefficient $|h_{X,Y}|^2$ is exponentially distributed with $\mathrm{E}\{|h_{X,Y}|^2\} = 1$. In addition, we assume that the network is interference-limited and thus the noise at the receiver is negligible. More formally, regarding a transmission from Node S_k to Node D_k, let x_{S_k} and x_{J_i} denote the normalized (unit power) symbol stream to be transmitted by S_k and its ith jammer J_i, respectively, P_{S_k} and P_{J_i} denote the corresponding transmission power. For an eavesdropper $E_i \in \xi$, the signal y_{E_i} received at E_i is given by:

$$y_{E_i} = \frac{\sqrt{P_{S_k}} h_{S_k,E_i}}{d_{S_k,E_i}^{\alpha/2}} x_{S_k} + \sum_{J_i \in \Phi_J} \frac{\sqrt{P_{J_i}} h_{J_i,E_i}}{d_{J_i,E_i}^{\alpha/2}} x_{J_i}, \quad (1)$$

where d_{S_i,E_i} (resp. d_{J_i,E_i}) denotes the distance between S_k (resp. J_i) and E_i, Φ_J denotes the set of jammers (*i.e.*, the simultaneous transmission nodes), and α is the path-loss exponent (typically between 2 and 6).

From the perspective of physical layer security, secure outage probability is an important security-related performance metric, which can be defined as follows:

Secrecy Outage Probability: The event of *secrecy outage* refers to the case when the SIR at one or more eavesdroppers is above a required threshold γ_E, such that the message can be decoded by the eavesdropper(s). The secrecy outage probability (SOP) P_{so} is defined as the probability the event of *secrecy outage* happens.

For a concerned ad hoc network, the SOP of a K-hop path $\Pi = \langle l_1, \ldots, l_K \rangle$ can be evaluated by

$$P_{so}(\Pi) = 1 - \exp\left(-\sum_{l_k \in \Pi} P_{S_k} \omega_k \right), \tag{2}$$

where $\omega_k = \frac{1}{\gamma_E} \sum_{i=1}^{|\mathcal{E}|} \frac{d_{J_i,E_i}^{\alpha}}{P_{J_i} d_{S_k,E_i}^{\alpha}}$. Please refer to [25] for the details.

3. DESIGN OF PCRR

In this section, we present the details of PCRR protocol design. PCRR is based on the framework of on-demand routing and mainly involves two modules, *i.e.*, routing establishment and routing maintenance, which will be elaborated sequentially.

3.1 Routing Establishment

In the routing establishment module, the classical AODV routing protocol uses the shortest path to transmit data to destination. However, the shortest path may not be the optimal one since eavesdroppers may near the shortest path and bottleneck nodes caused by traffic congestion often result in network performance deterioration. Motivated by this, in the process of establishing routing of PCRR, we first analyze the SOP of any available paths and choose the path meeting the end to end SOP constraint $P_{so}(\prod) \leq \sigma$ to ensure data security. Then, if there is more than one suitable path we adopt an end-to-end congestion relief scheme called ECR to choose the optimal one.

3.1.1 Route discovery

PCRR uses the reactive routing protocol frame. When traffic arrives, source node checks whether there is an existing route to its destination, if there is no such a route, source node broadcasts a RREQ message (route request message) to start route discovery process. Different from the traditional AODV routing, in PCRR routing, when the destination node receives a RREQ message, it does not reply the RREP message (route reply message) immediately to establish a route, but waits for a period of time to collect more RREQ messages and then selects the optimal route to reply the RREP message.

We consider a general multi-hop ad hoc network, where each node is equipped with

a single omni-directional antenna. An end-to-end path (route) $\Pi_i \in \Pi$ in the network is formed by $H(\Pi_i)$ links from a source node to its destination, where Π represents the set of all possible paths. We use $A(\Pi_i)$ to denote the maximum number of activated routes on path Π_i. In PCRR protocol, a RREQ message not only includes the information of hop count and the node address, but also indicates the maximum number of activated routes of nodes on this path for evaluating the possibility of congestion occurrence. Therefore, each node maintains a table to record the received RREQ messages, as shown in Table 1. We can see from Table 1 that each node collects the received RREQ messages and records $\max_{\Pi i \in \Pi} H(\Pi_i)$, $\max_{\Pi i \in \Pi} A(\Pi_i)$, $H(\Pi_{last})$ and $A(\Pi_{last})$, which represents the maximum hops to the destination node, the maximum number of activated routes on all paths, the hop count of the last received RREQ message, and the activated routes of the last received RREQ message, respectively.

Table 1. RREQ information in PCRR.

Source address	Sequence	$\max_{\Pi i \in \Pi} H(\Pi_i)$
$\max_{\Pi i \in \Pi} A(\Pi_i)$	$H(\Pi_{last})$	$A(\Pi_{last})$

3.1.2 Optimal path selection

In PCRR protocol, when a relay node receives the first arrived RREQ message, we use Π_1 to denote the path and record $H(\Pi_{last}) = H(\Pi_1)$, $A(\Pi_{last}) = A(\Pi_1)$, $\max_{\Pi i \in \Pi} H(\Pi_i) = H(\Pi_1)$ and $\max_{\Pi i \in \Pi} A(\Pi_i) = A(\Pi_1)$ into the routing table. Then, the first RREQ message will be forwarded to the next node. After that, if the relay node receives another RREQ message with the same sequence, the path is denoted by Π_2, the hop count is $H(\Pi_2)$ and the maximum number of activated routes on path Π_2 is $A(\Pi_2)$. If $H(\Pi_2) > H(\Pi_1)$, then $\max_{\Pi i \in \Pi} H(\Pi_i) = H(\Pi_2)$, otherwise, $\max_{\Pi i \in \Pi} A(\Pi_i) = A(\Pi_2)$. Based on the updated hop count and maximum number of activated routes on the path, we apply the following formula to calculate the routing metric $R_{metric}(\Pi_1)$ and $R_{metric}(\Pi_2)$ for Π_1 and Π_2, respectively.

$$R_{metric}(\Pi_i) = \beta \frac{A(\Pi_i)}{\max_{\Pi_i \in \Pi} A(\Pi_i)} + (1-\beta) \frac{H(\Pi_i)}{\max_{\Pi_i \in \Pi} H(\Pi_i)} \tag{3}$$

where β is a constant and $0 < \beta < 1$. It is worth noting that β can be regarded as the weights of congestion state and hop count in the route selection metric. The congestion state has a more important impact on the route selection process when we set a larger value of β. When we set $\beta = 1$, it indicates that the route selection is depended only on the congestion state of all possible routes; on the other hand, when we set $\beta = 0$, the route selection is depended only on the hop count, which reduces to the minimum hop routing scheme. Comparing $R_{metric}(\Pi_1)$ and $R_{metric}(\Pi_2)$, if $R_{metric}(\Pi_1) > R_{metric}(\Pi_2)$, the relay node forwards the new RREQ and update as $H(\Pi_{last}) = H(\Pi_2)$, $A(\Pi_{last}) = A(\Pi_2)$, otherwise, the new RREQ will be dropped.

For the destination node, it will wait a certain period of time after it receives the first RREQ message. We apply the formula (2) to check whether the SOP of every path meet the constraint $P_{so}(\Pi_i) \le \sigma$. If the constraint is not met, the RREQ will be dropped.

Otherwise, based on the route information from all the RREQ messages with the same sequence, we obtain $\max_{\Pi_i \in \Pi} H(\Pi_i)$ and $\max_{\Pi_i \in \Pi} A(\Pi_i)$. Furthermore, we apply the formula (3) to calculate the routing metric for each path, and then find the minimum one and reply the RREP message.

Here we provide an example to illustrate the routing establishment process of PCRR. As shown in Fig. 1, when relay node **4** receives the first RREQ message from node **3**, the hop count of path **S-3-4** is 2 and the maximum number of activated is 2, so we have $H(\Pi_{last}) = 2$, $A(\Pi_{last}) = 2$, $\max_{\Pi_i \in \Pi} H(\Pi_i) = 2$ and $\max_{\Pi_i \in \Pi} A(\Pi_i) = 2$, which are recorded in node **4**. After that, node **4** receives a new RREQ message through the path **S-6-7-4**. By updating the routing table, node **4** records that $\max_{\Pi_i \in \Pi} H(\Pi_i) = 3$ and $\max_{\Pi_i \in \Pi} A(\Pi_i) = 2$. We set $\beta = 0.5$, then the route metric of path **S-3-4** is $R_{metric}(\Pi_1) = 0.5 \times 1 + 0.5 \times 0.67 = 0.835$, while the route metric of path **S-6-7-4** is $R_{metric}(\Pi_2) = 0 + 0.5 \times 1 = 0.5$. It can be seen that $R_{metric}(\Pi_1) > R_{metric}(\Pi_2)$, so node **4** forwards the RREQ message which is from path **S-6-7-4**, and updates that $H(\Pi_{last}) = 3$ and $A(\Pi_{last}) = 0$.

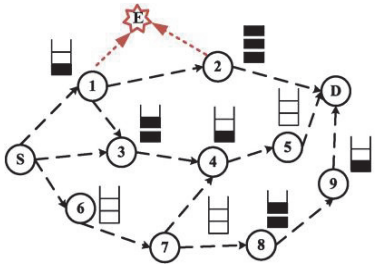


Fig. 1. Illustration for the routing establishment process of PCRR.

In Fig. 1, we assume that after the destination node **D** receives the first RREQ message from source node **S**, it waits for a period of time and receives RREQ messages from other three paths. We use Π_1, Π_2, Π_3 and Π_4 to denote the four paths **S-1-2-D**, **S-3-4-5-D**, **S-6-7-4-5-D** and **S-6-7-8-9-D**, respectively. We analyze this four paths' SOP, and find path **S-1-2-D** does not meet the constraint $P_{so}(\Pi_1) \leq \sigma$. This path is dropped by destination node **D** and then it records $\max_{\Pi_i \in \Pi} H(\Pi_i) = 5$ and $\max_{\Pi_i \in \Pi} A(\Pi_i) = 2$. The route metrics of these three paths are calculated respectively as follows:

$$R_{metric}(\Pi_2) = 0.5 \times 1 + 0.5 \times 0.8 = 0.9,$$
$$R_{metric}(\Pi_3) = 0.5 \times 0.5 + 0.5 \times 1 = 0.75,$$
$$R_{metric}(\Pi_4) = 0.5 \times 1 + 0.5 \times 1 = 1.$$

We can see that the metric of path Π_3 is the minimum. Therefore, PCRR protocol will choose this path, *i.e.*, **S-6-7-4-5-D**, to transmit data from the source node and destination node, and the destination node **D** will reply the RREP message through path Π_3.

3.2 Routing Maintenance

The basic operation of routing maintenance in PCRR is similar to that of the classical reactive routing protocols (AODV, *etc.*). Each node on the activated path will con-

firm the link state by periodically broadcasting Hello messages. If there is no response for three times, this node considers the link is broken and deletes the corresponding route information from its routing table. After that, the node sends a RRER message (route error message) to notice its neighbor nodes and upstream nodes to delete the route information about the broken link.

4. DESIGN OF M-PCRR

Based on the design of PCRR, we further propose a mixed-path end-to-end congestion relief physical layer routing protocol (M-PCRR). M-PCRR can decide whether the multi-path mechanism is activated according to the network status information.

In the case of eavesdropper far away the path, light traffic load and short average path length, M-PCRR operates the same as PCRR, while in case of eavesdropper near the relay nodes, overloaded traffic or long average path length, M-PCRR activates the multi-path mechanism such that the routing performance is expected to be better than that of PCRR. It can use the interference caused by multi-path simultaneous communication to make reception completely unintelligible. For the sake of clarity, we show the example of multi-path routing in in Fig. 2. Here, source node chooses two paths to transmit to destination node simultaneous. When relay node **1** sends data to node **3** and then to the destination node, source node and node **2** act as jammers, respectively and prevent eavesdropping on the two links. On the other hand, when relay node **2** sends data to destination, node **1** and **3** also act as jammers.

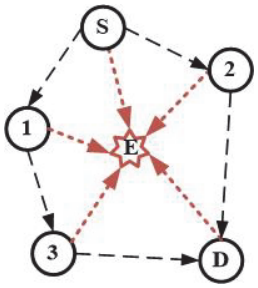


Fig. 2. Example multi-path with eavesdroppers.

In addition to adopting the routing table of PCRR, M-PCRR also includes a new multi-path routing table only in each source node, as shown in Table 2. The details of M-PCRR protocol are summarized as Algorithm 1.

Table 2. Multi-path routing table in M-PCRR.

Source address	Sequence	Hop count 1
Hop count 2	Next hop 1	Next hop 2
Route lifetime		

Here we provide an example to illustrate the routing establishment process of M-PCRR. As shown in Fig. 3, first we consider the network without eavesdropper.

Case 1: we consider that the source node **S** has traffic which is destined to node $\mathbf{D_1}$. M-PCRR starts route discovery operation and the destination node $\mathbf{D_1}$ receives two different RREQ messages from the paths **S-1-$\mathbf{D_1}$** and **S-2-$\mathbf{D_1}$**, respectively. Since both the paths are short (two hops) and the traffic load is light, source node **S** adopts the single-path routing strategy. By utilizing the ECR scheme, it chooses the path **S-1-$\mathbf{D_1}$** to transmit data.

Case 2: we consider that the source node **S** has traffic which is destined to node $\mathbf{D_2}$. Node $\mathbf{D_2}$ receives two different RREQ messages from the paths **S-2-3-$\mathbf{D_2}$** and **S-1-$\mathbf{D_1}$-$\mathbf{D_2}$**, respectively. Node $\mathbf{D_2}$ checks the hop count and traffic load of two paths. Although their hop counts are small, but both node **3** and node $\mathbf{D_1}$ are overloaded so that M-PCRR activates the multi-path mechanism. As a result, source node **S** transmits data to node $\mathbf{D_2}$ through both the paths **S-2-3-$\mathbf{D_2}$** and **S-1-$\mathbf{D_1}$-$\mathbf{D_2}$**.

Case 3: we consider that the source node **S** has traffic which is destined to node $\mathbf{D_3}$. Node $\mathbf{D_3}$ receives two different RREQ messages from the paths **S-2-3-$\mathbf{D_2}$-$\mathbf{D_3}$** and **S-4-5-6-7-8-$\mathbf{D_3}$**, respectively. Considering the eavesdropper and traffic load of two paths, for the path **S-2-3-$\mathbf{D_2}$-$\mathbf{D_3}$**, its hop count is small but the traffic is overloaded. For the path **S-4-5-6-7-8-$\mathbf{D_3}$**, its traffic is not overloaded but the hop count is large. Thus, both the paths do not meet the requirement of single-path routing strategy and M-PCRR activates the multi-path mechanism. As a result, the source node **S** transmits data to node $\mathbf{D_3}$ through both the paths **S-2-3-$\mathbf{D_2}$-$\mathbf{D_3}$** and **S-4-5-6-7-8-$\mathbf{D_3}$**.

Algorithm 1: M-PCRR protocol

1: The destination node waits for a period of time to collect several RREQ messages, and check whether there are eavesdroppers near the paths. Then it finds the path with the minimum R_{metric}.
2: **if** The minimum R_{metric} is less than the given threshold value **and** eavesdropper far away the path with minimum R_{metric} **then**
3: The destination node executes **Program 1**.
4: **else**
5: The destination node executes **Program 2**, *i.e.*, the multi-path mechanism.
6: **end if**

Program 1: Single-path scheme

1: The destination node chooses the path with minimum R_{metric} to reply the RREP message.
2: When a relay node receives the RREP message, it updates the routing table and establishes the path to the destination node.
3: When the source node receives the RREP message, it starts to transmit data through the established path.

Program 2: Multi-path mechanism

1: The destination node chooses the path with minimum R_{metric} to reply the RREP message.
2: The destination node randomly chooses another path P_{spare} which on the other side of the eavesdropper and is different from the path with minimum R_{metric}, and reply the RREP message through this path.
3: When the source node receives the second RREP message, it activates the multi-path routing table and updates the related routing information.
4: The source node starts to transmit data and distributes the traffic flow to both the paths.

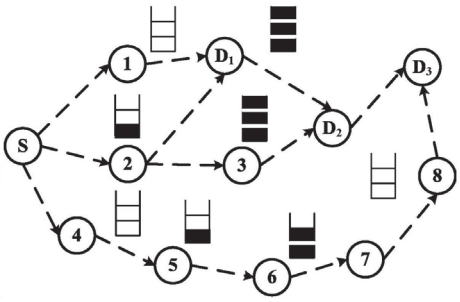


Fig. 3. Illustration for the routing establishment process of M-PCRR without eavesdropper.

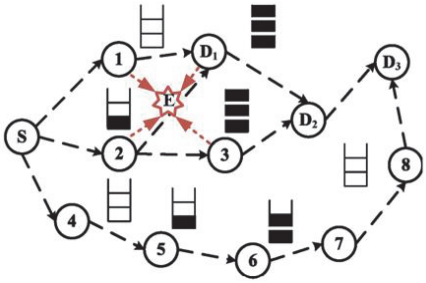


Fig. 4. Illustration for the routing establishment process of M-PCRR with eavesdropper.

Then, we consider the network with an eavesdropper which is shown in Fig. 4.

Case 4: we consider that the source node **S** has traffic which is destined to node $\mathbf{D_1}$. M-PCRR starts route discovery operation and the destination node $\mathbf{D_1}$ receives two different RREQ messages from the paths **S-1-$\mathbf{D_1}$** and **S-2-$\mathbf{D_1}$**, respectively. Although both the paths are short (two hops) and the traffic load is light, there is an eavesdropper near node **1**, **2**, **3** and $\mathbf{D_1}$. Therefore, source node **S** adopts the multi-path routing strategy. It chooses both path **S-1-$\mathbf{D_1}$** and **S-2-$\mathbf{D_1}$** to transmit data.

Case 5: we consider that the source node **S** has traffic which is destined to node $\mathbf{D_2}$. Node $\mathbf{D_2}$ receives two different RREQ messages from the paths **S-2-3-$\mathbf{D_2}$** and **S-1-$\mathbf{D_1}$-$\mathbf{D_2}$**, respectively. Because the eavesdropper and traffic load of two paths, M-PCRR activates the multi-path mechanism. As a result, source node S transmits data to node $\mathbf{D_2}$ through both the paths **S-2-3-$\mathbf{D_2}$** and **S-1-$\mathbf{D_1}$-$\mathbf{D_2}$**.

Case 6: we consider that the source node **S** has traffic which is destined to node $\mathbf{D_3}$. Node $\mathbf{D_3}$ receives three different RREQ messages from the paths **S-1-$\mathbf{D_1}$-$\mathbf{D_2}$-$\mathbf{D_3}$**, **S-2-3-$\mathbf{D_2}$-$\mathbf{D_3}$** and **S-4-5-6-7-8-$\mathbf{D_3}$**, respectively. For the path **S-1-$\mathbf{D_1}$-$\mathbf{D_2}$-$\mathbf{D_3}$** and **S-2-3-$\mathbf{D_2}$-$\mathbf{D_3}$**, their hops are small but relay nodes near the eavesdropper and traffic is overloaded. For the path **S-4-5-6-7-8-$\mathbf{D_3}$**, their relay nodes far away the eavesdropper, traffic is light but the hop count is large. Thus, those paths do not meet the requirement of single-path

routing strategy and M-PCRR activates the multi-path mechanism. As a result, the source node **S** transmits data to node $\mathbf{D_3}$ through the three paths **S-1-D_1-D_2-D_3**, **S-2-3-D_2-D_3** and **S-4-5-6-7-8-D_3**.

5. SIMULATION RESULTS

As described in previous sections, the motivations of our proposed routing protocols PCRR and M-PCRR are two-folds. On one hand, they aim to relieve the end-to-end traffic congestion in ad hoc networks; on the other hand, they are physical layer security-aware to prevent data transmission from eavesdropping attacks. Therefore, in this section, we first conduct extensive experiments with OPNET network simulator in none eavesdropper environment to compare the performance among PCRR, M-PCRR and the most typical routing protocol in ad hoc networks, *i.e.*, AODV. The performance metrics include throughput, end-to-end delay, control overhead and hop count, and the simulation results are summarized in Figs. 5-8, respectively. In these experiments, we set that the network size is 1000×1000, the number of nodes is 100, the packet length is 1000 bits and the channel rate is 1 Mb/s. The random waypoint mobility model is applied and the maximum node speed is 1 m/s. The source-destination pairs are generated according to the model in [34].

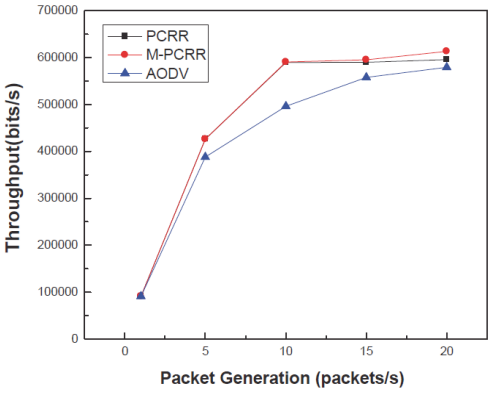


Fig. 5. Throughput performance.

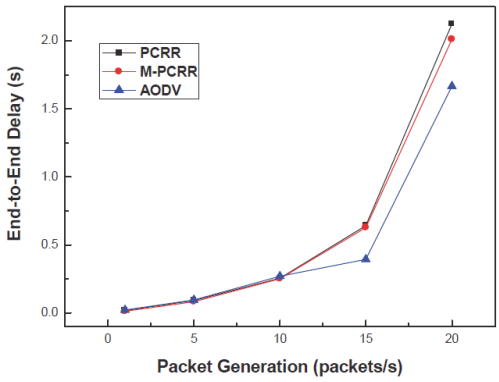


Fig. 6. End-to-end delay performance.

Fig. 5 summarizes that how the throughput performance varies with packet generation rate. We can see from Fig. 5 that, PCRR can achieve a higher throughput than AODV under the light traffic load scenario. As the packet generation rate increases, the gap deceases and diminishes to a small value when the packet generation rate is up to 20 packets/s. The throughput performance of M-PCRR is similar to that of PCRR under the light traffic load environment. However, it can achieve a better throughput under the heavy traffic load environment. This is because that when the network traffic is not overloaded, PCRR can find an idle path or a path with light traffic load to transmit data, such that the bandwidth resource utilization can be increased and the successful packet delivery rate can be improved. As the packet generation rate increases, all the nodes in

network are overloaded so that PCRR can't find a suitable path to improve the throughput performance, and thus the benefits of PCRR reduces and the throughput performance approaches to that of AODV. By activating the multi-path routing mechanism, M-PCRR can achieve a better load balance, such that the throughput performance under the heavy traffic load scenario is better than that of PCRR and AODV.

Fig. 6 summarizes the end-to-end delay performance. We can see that when the network load is not heavy, end-to-end delay performance of the three routing protocols is similar to each other. However, with traffic load increasing, AODV can achieve a shorter delay than PCRR and M-PCRR. This is because that when the network is close to be overloaded, that is to say, almost all available paths are congested, PCRR tends to select a path with small hop count but this path could be heavily congested, which results in a large end-to-end delay. On the contrary, AODV always follows the first come first served principle such that the selected path has a shortest delay. M-PCRR activates the multi-path routing mechanism under the heavy traffic load environment which serves as a tradeoff between PCRR and AODV, thus the end-to-end delay performance of M-PCRR is better than that of PCRR but worse than that of AODV.

Fig. 7 summarizes the control overhead of the three routing protocols. We can see that the control overhead of PCRR and M-PCRR is almost the same as that of AODV, which indicates that our proposed PCRR and M-PCRR can relieve the network congestion and improve the network throughput, while without increasing the control overhead.

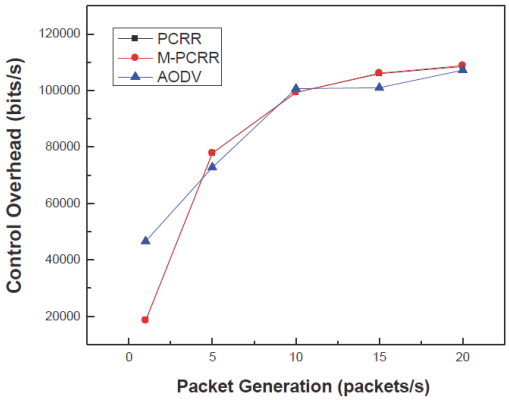


Fig. 7. Overhead performance.

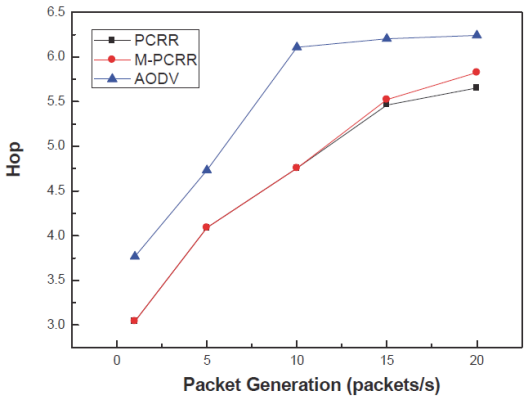


Fig. 8. Hop count versus packet generation rate.

Fig. 8 summarizes the path hop count of the three routing protocols. We can see that under the light traffic load scenario, the path hop count of PCRR is similar to that of M-PCRR, but less than that of AODV. Under the heavy network load environment, the path hop count of M-PCRR becomes larger than that of PCRR but also less than that of AODV. This is because that in such a case all paths are congested, R_{metric} of a path is dominated by its hop count according to formula (3). Thus, PCRR choosing the path with minimum R_{metric} is equivalent to choosing the path with minimum hop count. M-PCRR not only uses the path with minimum R_{metric} but also another longer path to transmit data, so the path hop count of M-PCRR is larger than that of PCRR.

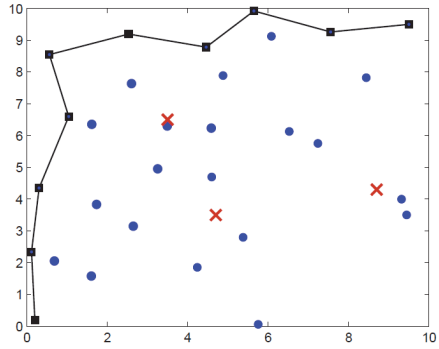


Fig. 9. Illustration of route selection with PCRR.

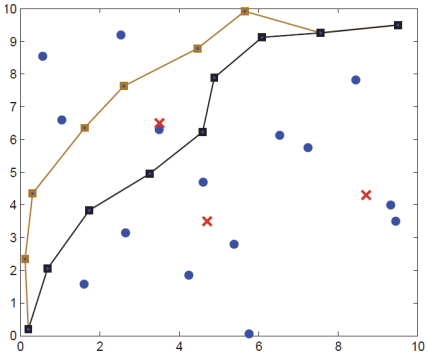


Fig. 10. Illustration of route selection with M-PCRR.

Regarding the aspect of transmission security, we further illustrate in Figs. 9 and 10 that how the route selection is conducted in an ad hoc network with PCRR and MPCRR routing protocols when eavesdroppers exist. Since AODV has no consideration of security, it executes the same route selection procedure under both the scenarios without and with eavesdropper(s), and thus is neglected for simplicity. We consider a multi-hop ad hoc network where 30 legitimate nodes (shown by blue dots and blocks) are placed randomly in a 10×10 square area. The source node is placed at the lower left corner and the destination is placed at the upper right corner. We strategically place 3 eavesdroppers (shown by red "×") in the center of this area to gain more insights into the route selection process. The selected route(s) is denoted by the connected blocks.

We can see from Figs. 9 and 10 that when there exist some eavesdroppers in the network, PCRR chooses the path which has long path length but is far away from the eavesdroppers to satisfy the SOP requirement. M-PCRR chooses two paths whose path length is shorter than that of PCRR, this is because that M-PCRR utilizes the interference from simultaneous transmissions of these two paths to make reception completely unintelligible. It indicates that M-PCRR can achieve a better performance under the security constraint.

6. CONCLUSIONS

In this paper, we studied the routing protocol design for ad hoc networks. We first proposed a physical layer security-aware congestion relief routing protocol (PCRR) based on sensing the hop count and congestion state of available paths. By combining the advantages of single-path and multi-path routing strategies, we then extended PCRR to a mixed-path version, M-PCRR, which can decide whether or not to execute the multi-path mechanism according to the current network state information. Extensive OPNET simulations have been conducted to verify that PCRR and M-PCRR can improve the network throughput, reduce the path hop count, while ensuring the end-to-end delay and control overhead. In our future research, we will establish a real ad hoc network consisting of single-board computers, and realize the routing protocols in the network to conduct performance experiments.

ACKNOWLEDGMENT

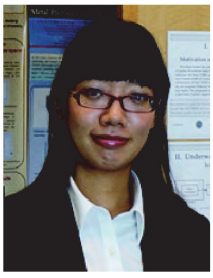
This work was supported in part by the University Fundamental Research Foundation of China JBX170612, in part by the Project of Cyber Security Establishment with Inter University Cooperation, in part by the Secom Science and Technology Foundation, and in part by the Recruitment Program of Foreign Experts MS2016XADZ046.

REFERENCES

1. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, Vol. 54, 2010, pp. 2787-2805.
2. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, Vol. 29, 2013, pp. 1645-1660.
3. L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, Vol. 10, 2014, pp. 2233-2243.
4. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, Vol. 17, 2015, pp. 2347-2376.
5. C. Public, "Cisco visual networkingindex: Forecast and methodology, 2016-2021," *Cisco White paper*, 2017.
6. K. Zhao and L. Ge, "A survey on the internet of things security," in *Proceedings of the 9th International Conference on Computational Intelligence and Security*, 2013, pp. 663-667.
7. T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proceedings of IEEE/ACM International Conference on Computer Aided Design*, 2014, pp. 417-423.
8. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: Perspectives and challenges," *Wireless Networks*, Vol. 20, 2014, pp. 2481-2501.
9. D. G. Reina, S. L. Toral, F. Barrero, N. Bessis, and E. Asimakopoulou, "The role of ad hoc networks in the internet of things: A case scenario for smart environments," *Internet of Things and Inter-Cooperative Computational Technologies for Collective Intelligence*, Springer, 2013, pp. 89-113.
10. M. Conti and S. Giordano, "Mobile ad hoc networking: milestones, challenges, and new research directions," *IEEE Communications Magazine*, Vol. 52, 2014, pp. 85-96.
11. J. Loo, J. L. Mauri, and J. H. Ortiz, *Mobile Ad Hoc Networks: Current Status and Future Trends*, CRC Press, FL, 2016.
12. B. Schneier, "Cryptographic design vulnerabilities," *Computer*, Vol. 31, 1998, pp. 29-33.
13. W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, Vol. 53, 2015, pp. 16-20.

14. A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, Vol. 103, 2015, pp. 1747-1761.
15. A. Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L. Bölöni, and D. Turgut, "Routing protocols in ad hoc networks: A survey," *Computer Networks*, Vol. 55, 2011, pp. 3032-3080.
16. E. Alotaibi and B. Mukherjee, "A survey on routing algorithms for wireless ad-hoc and mesh networks," *Computer Networks*, Vol. 56, 2012, pp. 940-965.
17. C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," *IETF RFC 3561*, July, 2003.
18. D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, 1996, pp. 153-181.
19. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in *Proceedings of IEEE International Multi-Topic Conference*, 2001, pp. 62-68.
20. W. Saad, X. Zhou, B. Maham, T. Basar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multi-hop networks," *IEEE Transactions on Wireless Communications*, Vol. 11, 2012, pp. 3980-3991.
21. M. Ghaderi, D. Goeckel, A. Orda, and M. Dehghan, "Minimum energy routing and jamming to thwart wireless network eavesdroppers," *IEEE Transactions on Mobile Computing*, Vol. 14, 2015, pp. 1433-1448.
22. J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Transactions on Communications*, Vol. 64, 2016, pp. 753-764.
23. J.-H. Lee, "Optimal power allocation for physical layer security in multi-hop df relay networks," *IEEE Transactions on Wireless Communications*, Vol. 15, 2016, pp. 28-38.
24. Y. Xu, J. Liu, Y. Shen, X. Jiang, and T. Taleb, "Security/qos-aware route selection in multi-hop wireless ad hoc networks," in *Proceedings of IEEE International Conference on Communications*, 2016, pp. 1-6.
25. Y. Xu, J. Liu, O. Takahashi, N. Shiratori, and X. Jiang, "SOQR: Secure optimal qos routing in wireless ad hoc networks," in *Proceedings of IEEE Wireless Communications and Networking Conference*, 2017, pp. 1-6.
26. Y. Xu, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Physical layer security-aware routing and performance tradeoffs in ad hoc networks," *Computer Networks*, Vol. 123, 2017, pp. 77-87.
27. H. Han, S. Shakkottai, C. V. Hollot, R. Srikant, and D. Towsley, "Multi-path tcp: a joint congestion control and routing scheme to exploit path diversity in the internet," *IEEE/ACM Transactions on Networking*, Vol. 14, 2006, pp. 1260-1271.
28. G. Carofiglio, M. Gallo, L. Muscariello, and M. Papali, "Multipath congestion control in content-centric networks," in *Proceedings of IEEE INFOCOM Workshops*, 2013, pp. 363-368.
29. P. Sermpezis, G. Koltsidas, and F.-N. Pavlidou, "Investigating a junction-based multipath source routing algorithm for vanets," *IEEE Communications Letters*, Vol. 17, 2013, pp. 600-603.

30. X. Huang and Y. Fang, "Performance study of node-disjoint multipath routing in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, Vol. 58, 2009, pp. 1942-1950.
31. X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Transactions on Wireless Communications*, Vol. 10, 2011, pp. 2764-2775.
32. Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, Vol. 31, 2013, pp. 2099-2111.
33. A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, Vol. 16, 2014, pp. 1550-1573.
34. N. Zhou, H.Wu, and A. A. Abouzeid, "The impact of traffic patterns on the overhead of reactive routing protocols," *IEEE Journal on Selected Areas in Communications*, Vol. 23, 2005, pp. 547-560.



Yang Xu (徐揚) received the B.E. degree in Communications Engineering and the Ph.D. degree in Communication and Information Systems from Xidian University, Xi'an, China, in 2006 and 2014, respectively. She is currently a Lecturer at the School of Economics and Management, Xidian University, and also a visiting scholar in Future University Hakodate. She has published about 15 papers at premium international journals and conferences, including IEEE Transactions on Wireless Communication, Computer Networks, Ad Hoc Networks, Wireless Networks, IEEE ICC and IEEE WCNC. Her current research interests include physical-layer security, blockchain and wireless communications.

Jia Liu (劉佳) received his Ph.D. degree in 2016, from the School of Systems Information Science, Future University Hakodate, Japan. He is currently an Assistant Professor in the Center for Cyber Security Research and Development, National Institute of Informatics, Japan. His research interests include mobile ad hoc networks, 5G communication systems, D2D communications, cyber security, *etc.* He has published about 15 technical papers at premium international journals and conferences, like IEEE Transactions on Wireless Communication, Computer Networks, Ad Hoc Networks, Computer Communications, IEEE ICC and IEEE WCNC.

Ruo Ando (安藤類央) has received Ph.D. from Keio University in 2006. He is now an Associate Professor by special appointment of National Institute of Informatics since 2016. His research interests focus on network security, information security and big data mining technologies. He was engaged in Driver ware project supported by US Air Force Office of Scientific Research with Grant Number AOARD 03-4049 in 2005-2006. He received Outstanding Leadership Award in the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC-09) at China in 2009. He is the member of Trusted Computing Group JRF (Japan Regional Forum) in 2008-2015. He received research paper award of Internet conference in 2013. He has presented in many security conferences such as SysCan 2009, FrHack 2009, AVTokyo 2009, DeepSec 2009, PacSec Tokyo 2011, GreHack 2013. He served as reviewer of Springer Journal PPNA, Willey Journal of Security and Communications Networks and IEEE transactions of Information Forensics and Security. He worked in project "Next Generation Security Info-Security R&D" METI (FY2008-10). He was engaged in project "Unknown malware detection using incremental malware detection" MEXT (FY2012-2015).

Norio Shiratori (白鳥則郎) is currently an Emeritus and Research Professor at the RIEC (Research Institute of Electrical Communication), Tohoku University, Japan. He is also a board member of Future University of Hakodate and a Visiting Professor of Chuo University, Japan. He is a Fellow of the IEEE (Institute of Electrical and Electronic Engineers), the IPSJ (Information Processing Society of Japan) and the IEICE (The Institute of Electronics, Information and Communication Engineers). He was the President of the IPSJ from 2009 to 2011. He has published more than 15 books and over 400 refereed papers in computer science and related fields. He was the recipient of the "IPSJ Memorial Prize Winning Paper Award" in 1985, the Telecommunication Advancement Foundation Incorporation Award in 1991, the "Best Paper Award of ICOIN-9" in 1994, the "IPSJ Best Paper Award" in 1997, and many others including the most recent "Outstanding Paper Award of UIC-07" in 2007.